ARTIFICIAL INTELLIGENCE APPROPRIATE USE POLICY

A. Purpose

The purpose of this policy is to establish guidelines that ensure responsible and secure use of Artificial Intelligence (AI) by Inyo County employees. Inyo County recognizes the value of AI to increase efficiency, improve processes, and enhance services. Simultaneously, the County expects that AI is used in an appropriate and ethical manner which ensures information security, respects privacy, and does not compromise the integrity of work product.

B. Scope

This policy applies to all employees, contractors, and third-party individuals or entities who have access to AI technologies or use AI tools on behalf of Inyo County.

C. Definitions

Artificial Intelligence (AI): The simulation of human intelligence processes by machines, including problem-solving and decision-making.

Generative AI Tools: Specialized tools that are a specific subset of artificial intelligence focused on creating new content, such as text, images, videos, music, and more.

PHI: Protected Health Information

PII: Personally Identifiable Information

D. Use of AI Systems

1. **Policy Compliance:** All users of AI systems must be familiar with this policy and exercise sound judgment in their AI use. They must have completed assigned training for approved AI system(s) and agree to complete any future training assigned.
2. **Use of County Email Address:** When registering for AI services, use official County email addresses for security and accountability.
3. **Authorized AI Tools:** Only those AI tools approved by the Information Services Department may be used, as referenced in Inyo County Approved AI Tools document. Use of additional tools must be obtained via Information Services and the Department Head prior to actual use.
4. **Reporting Concerns:** Report any issues or concerns regarding AI tool usage to your supervisor or the Information Services Department.
5. **Additional Rules:** Departments may establish specific guidelines for AI usage tailored to their needs. In particular, departments that deal with a lot of PII and PHI are expected to train their employees on the perils of inadvertent exposure of private information.

E. Expectations Around Responsible AI Use

Employees may integrate AI into their work where its use is seen as beneficial, while ensuring the security of sensitive information and compliance with County policies. Key principles include:

1. **Data Privacy and Security:** AI use must comply with all relevant data privacy standards, including the Health Information Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), Internal Revenue Services (IRS) regulations, and the California Consumer Privacy Act (CCPA).

   All AI tools and prompts shall be treated as if they are publicly visible, and in no case may PII, PHI or any other sensitive information be entered into AI prompts or systems.

2. **User Training:** Employees must participate in AI training provided by the County prior to using any such tools to ensure appropriate usage and compliance with policies.

3. **Preemptive Approval:** Before any AI tools may be used by any County employee or representative, prior approval must be obtained from their Department Head. County users must have plug-ins or other 3rd-party tools reviewed and approved by the Information Services Department as well as your own department before they may be used.

4. **Responsible Use:** County personnel shall use AI tools ethically and in alignment with County values and policies.

5. **Decision Making:** AI tools shall not be used as the sole input for drafting documents, establishing policy, developing staff recommendations, or decision-making efforts. However, AI tools may be used to assist in these processes so long as information provided is further researched and critiqued. A final human check is required.
   a. **Transparency:** The use of AI systems for the creation of work products or applications where the output is presented should be explainable. Clearly indicate when AI significantly contributed to a work product and provide appropriate citations for its use.
   b. **Informed Consent:** The public must be informed when interacting with AI tools and have an option to opt-out of using AI.
   c. **Accountability:** Employees and contractors acknowledge that AI systems can make errors. They can be leveraged to gather input. But the person in charge is responsible for ensuring the accuracy of the data and the decision.

6. **Avoiding Bias & Hallucinations:** As a user of AI, you are responsible for content generated. AI tools may generate biased outputs. Regularly review AI-generated content to ensure fairness and accuracy, and review the output for hallucinations (i.e., content fabricated by generative AI).

Cautions Regarding Third-Party Risks

1. **Use of AI Plugins:** Employees should avoid the use of AI plugins and browser extensions. Many extensions automatically upload the content of the page they are on to third-party servers which may inadvertently expose sensitive information. Employees should have plugins approved by the Information Services department prior to using them.

2. **Viewing Sensitive Information:** Never view PII or PHI while AI plugins are in use, as this may risk unintentional data exposure.

3. **Data Leakage Risks:** Be aware that other AI tools may also upload information without user consent. Always review the privacy policies and data handling practices of any AI tool before use and avoid entering sensitive or confidential information into these systems. If in doubt, please request assistance from IS.

F. Accountability

Employees are responsible for the quality and compliance of all AI-generated content used in their work. The County will regularly monitor the use of AI to ensure they meet security and risk management criteria.

G. Prohibited Uses

1. **Unauthorized Access:** Do not use AI tools to access data or systems without authorization from Information Services.

2. **Sensitive, Protected, and Confidential Information:** Never enter PII or PHI or any other sensitive information into AI systems. No AI tool currently meets the County's security standards for handling sensitive information.

3. **Unlawful Activities:** AI must not be used for illegal, harmful, or malicious activities.

4. **Personnel Decisions:** AI should not be used for decisions related to hiring, promotions, separation, benefits, or other sensitive matters.

I. Term

The County will review and update this policy at lease once every 12 months to keep it aligned with ethical and legal standards as well as technological advancements.

ARTIFICIAL INTELLIGENCE APPROPRIATE USE POLICY

Approved AI Tool List

Only the follow AI tools approved by the Information Services Department may be used for county business.

- **Microsoft Copilot** hosted on the government cloud and deployed by the information services department